Guidelines for Policies and Procedures Regarding Electronic Communication Technology

Executive Fire Officer Program
Executive Development

BY: Phil Quinton
Fire and Emergency Services
City of Alpharetta, Georgia

An applied research project submitted to the National Fire Academy
as part of the Executive Fire Officer Program

August 12, 1999

Abstract

The purpose of this evaluative research paper was to explore the issue of electronic communication technology, specifically the Internet and e-mail, as it relates to the Department of Fire and Emergency Services of the City of Alpharetta, Georgia. The problem identified in this paper, is that with the spread of this technology, there is a potential for conflict between an employee's perceived right to communication privacy and free speech versus the desire of the employer (City, County or State) to support a controlled and productive work environment.

Three research questions were asked. What is the nature, scope and cost of Internet and e-mail abuse in the workplace? Does an employer have a legal right to restrict, monitor, filter and control employee Internet and e-mail usage? What would constitute a reasonable and legally enforceable policy regarding Internet and e-mail use in the fire service and what elements should be included in such a policy?

To answer these questions, local city and county information management department representatives were surveyed, national statistics were reviewed, and questionnaires were distributed to employees to determine their perceptions of existing Internet and e-mail polices and procedures. Court decisions affecting this issue were then examined and compared with existing policies of the City of Alpharetta, and an examination of technologies designed to overcome some forms of Internet and E-mail abuse was conducted. Finally, websites of special interest groups, which either support or oppose Internet content blocking, were reviewed.

Results indicated that the existing policies and procedures of the City of Alpharetta Department of Fire and Emergency Services are within the law as regards to monitoring, and blocking of electronic communications. Further, the existing polices and procedures are consistent with other local area governments. This applied research paper did reveal that the Department might not be in full compliance with the requirements of the law regarding written policies, or in the procedures for informing and training employees regarding these policies and procedures.

It was recommended that existing policies and procedures be revisited and rewritten. Employees should be transitioned to the new policies and procedures by a training program in which their legal rights and responsibilities are discussed. This training should be conducted in an open and sensitive manner through a series of informational workshops, and an updated employee manual that reflects these changes should be distributed. Employee concerns and feedback should be considered.

Table of Contents

Abstract Page ii

Table of Contents Page iv

Introduction Page 1

Background and Significance Page 2

Literature Review Page 8

Procedures Page 14

Results Page 18

Discussion Page 28

Recommendations Page 33

References Page 39

Table One - Survey of Policies of Local Area Governments Page 27

Appendix One Page 42

Introduction

An area of growing controversy, and concern to Fire Service Administrators is electronic communication technology, specifically electronic mail (e-mail) and the Internet. The advantages of using electronic communication technology in the fire service are many and growing. It is an efficient method of communication among firefighters at different stations or from the stations to the departmental or administrative complexes. An electronic network allows for instant receiving and sending of data and empowers employees to engage in rapid and reliable communication. The presence of e-mail, and the Internet in Fire Stations, however, has created problems that Fire Chiefs only a few years ago did not face.

The problem is that with the spread of electronic communication technology, there is an increased potential for conflict between an employee's perceived right to communication privacy and free speech versus the desire of the employer (City, County or State) to support a controlled and productive work environment. The purpose of this Executive Fire Officer research paper was to explore the issue of Internet and E-mail use in the City of Alpharetta Department of Fire and Emergency Services and to provide a framework for developing clear and enforceable polices regarding Internet and e-mail usage by employees.

This research paper utilizes the evaluative method, and the following specific questions are considered:

1. What is the nature, scope and cost of Internet and e-mail abuse in the workplace?
2. Does an employer have a legal right to restrict, monitor, filter and control employee Internet and e-mail usage?

3. What constitutes a reasonable and legally enforceable policy regarding Internet and e-mail use in the workplace and what basic elements should be included in such a policy?

Background and Significance

While no single individual can be credited with inventing the various electronic communication technologies that we know today as the Internet and e-mail, the beginnings are generally traced to the early days of the cold war. The United States military was investigating how people could communicate after the expected devastation of a nuclear attack or natural disaster. An outbreak of a nuclear war would require a command and control network, linking the nation and the world. Such a communications network would however, be vulnerable as an obvious first strike target (Sterling.)

The defense requirements included that the system be totally decentralized with no controlling authority or central communication centers. It had to be flexible, so if any part of the network collapsed, the system could continue to operate. The individual parts of the network would be potentially unreliable, therefore the system must be able to overcome its own unreliability (Sterling.)

In this system, all units would be equal to all other units, each able to originate, pass and receive messages. The messages themselves would be divided into information packets; each packet would be separately addressed and would work its way through the system independent and separate from any other packet. Each information packet would begin at a specified source and end at a designated location, but the information would follow different paths as it worked its way through the network. In fact, the route that any specific information might take would be irrelevant. The information would be transferred from unit to unit to unit in the general direction of its destination until it ended up at the intended point (Sterling.)

If any part of the network were lost to enemy action or natural disaster, there would be no interruption in the flow of information. The packets would simply abandon the destroyed paths and move to unaffected paths along the network.

The solution developed by military researchers evolved over time into the present forms of electronic communications technology, often called the World Wide Web. This network includes the Internet and E-mail systems (December and Randall 1997.)

Aside from military use, it was realized that there was a potential for this network of computers to be used for business and educational purposes. Personal computers did not yet exist and rented computer time was expensive, therefore, the opportunity to link computers together for shared information created interesting possibilities (Sterling.)

Soon, users began to modify the network into a high-speed electronic post-office. The largest category of information exchanged was not, as originally conceived, collaboration on scientific projects, exchange of technical information, notes on research and long-distance computer sharing. Instead, it was most often used for news and personal messages. Not only were people using the system for personal communication, but also developing and providing this service was becoming a major industry (Sterling).

As the use of personal computers increased, many individuals, as well as businesses, social, religious, political and special interest groups gained possession of reasonably priced, but powerful computers. Technology made it easy to link these computers into the growing network. This system of inter-related networks came to be known as the "Internet."

Commercial and Business usage of the Internet grew slowly at first. In 1971, there were twenty-three host machines, by 1980 there were approximately one hundred connected computers, and in 1990 there were over one hundred thousand. By 1994, the number of systems connected to the Internet exceeded one million and by 1997 an estimate placed the number of users at well over twenty-five million (December and Randall 1997.)

By 1998, the Internet was growing at a rate of twenty percent a month. According to best estimates, the number of machines connected to the Internet is now doubling every year (Sterling).

The Internet currently contains millions of documents, with thousands added each day, and due to the ease with which data can be added or modified, the information is constantly changing. Links from one computer to another and from one document to another across the network unify the Internet into a single information system.

What is the value to the general public of being connected to the World Wide Web? One reason for some people is freedom. There is no controlling authority or agency over this technology. There are no censors or government regulators looking over your shoulder as you "surf the Web." In principle, any unit can speak openly and freely to any other unit, as long as a few basic laws against society such as child pornography or openly criminal activities are not violated.

Another advantage of the World Wide Web is that it is inexpensive to use. At the present time, the World Wide Web as a whole doesn't charge for long-distance service or for access time. In fact, since the “Internet” itself doesn’t officially exist as an entity, “it” cannot charge for anything. Each group of people accessing the Internet is responsible for their own machine and their own section of line.

What is the value to the City of Alpharetta, and to the Department of Fire and Emergency Services to be connected to the Internet and to use e-mail? The City of Alpharetta is a suburban community just north of Atlanta. In 1980, the population was less than 4,000 people, and there were about 30 city employees. By 1990, there were over 13,000 citizens and around 150 employees. However, since 1990, the population has increased to around 30,000 citizens, nearly 30 million square feet of office space has been constructed, and over 1,000 retail businesses have moved in. It is now estimated that the daytime service population can often reach 100,000 people (B. Patton, Department of Community Development, personal communication, April. 26, 1999).

The City is located in a high-tech environment, with such local employers as Nortel Networks, Digital Equipment Corporation, Lucent Technologies, Ryder Transportation Data Center, G. E. Capital, and Siemens Energy and Automation (B. Patton, Department of Community Development, personal communication, May. 2, 1999).

Approximately 350 people are now employed by the city on a full time basis. These are organized into twelve city departments including Administration, Community Development, Finance, Purchasing, Information Services, Human Resources, Inspections and Permits, Engineering, Parks and Recreation, Public Works, Police, and Fire and Emergency Services. The workforce is diverse in regards to education, age, race, and gender. Some employees have a high level of computer efficiency and background expertise (B. Busby, Department of Human Resources, personal communication, June 1999).

A vital operation within the City of Alpharetta is the Department of Fire and Emergency Services. In 1990, the Fire Department (as it was then officially known) was an all-volunteer group of about 30 people working out of one fire station. Today, there are 75 firefighters operating nine pieces of first line apparatus out of five strategically placed fire stations. Fewer than 20% of the career firefighters employed by the City of Alpharetta have more than five years of employment and the average age of the Firefighters is 28 years (Alpharetta Fire and Emergency Services, Annual Report, 1997.)

There are 130 computer desktop workstations in use throughout all City departments and these are all networked together into a single system. All of these have E-mail capability while only 33 of the 130 are Internet accessible. E-mail accessibility was phased in on a department by department basis over a two to three year period. All employees of the City now have an assigned E-mail address regardless of their immediate computer access. Until January 1999, Internet accessibility was limited to the Information Services Department. At that time, it was expanded to other departments at the discretion of the individual department head. (Mullis, Robert, Director, Information Services Department, personal communication, April 26, 1999.)

The current policies regarding Internet and e-mail usage for the Department of Fire and Emergency Services and the City as a whole consist of two documents in memo form, and transmitted to employees by e-mail only. The first document is a general list of do’s and don’ts regarding Internet and e-mail usage. It was e-mailed to various departments and posted on bulletin boards. At the time of this writing a copy was not available within the Department of Fire and Emergency Services, however a copy was obtained from the MIS Department and when examined, several problems were noted. Among these was that there was no indication of the date of issue, it was not on City of Alpharetta letterhead and it was signed only by the MIS Director which raised a question regarding his authority to set policy over other city departments. Upon investigation, it was found that existing city policies were mute on that issue.

The second document deals with the Internet blocking system (Surfwatch), its parameters, and contains a list of categories that are blocked. Among the blocked categories are sexually explicit, violence, hate speech, gambling, drugs, firearms, alcohol, tobacco, astrology, mysticism, games, glamour, intimate apparel, hobbies, and job search. Also blocked are personal adds, dating, real estate, shopping, sports, and chat lines. Among the unblocked categories are general news, investment, motor vehicles, and travel. This memo ends by saying that since any of these categories can be logged and monitored, employees should use "good judgement" in accessing the Internet. (E-mail message from Robert Mullis MIS Director, July 20, 1999)

As with the first document, it had no indication of the date of issue and was not on City of Alpharetta letterhead. And again, it was signed by the MIS Director. But most significantly, both documents were transmitted to intended employee recipients by e-mail. This leaves questions as to who may or may not have received it.

This research topic is relevant to the Executive Fire Officer Program, because in order to achieve a position of responsibility within the modern fire service, a senior fire executive must demonstrate skills in areas such as fire prevention and suppression. Beyond that, however, it is critical that fire executives be aware of the changing legal, social and cultural environment that technology can create and how changing technology can affect decisions, procedures and policies.

Literature Review

Just as a building must be constructed from the foundation, so must an Executive Fire Officer Program applied research paper have a solid foundation upon which it is based. This researcher approached the subject of electronic communication technology, as represented by the Internet and e-mail, from a background of limited prior computer knowledge, having for the first time surfed the Internet and sent an e-mail message less than three months prior to commencing this research.

This research began with a survey of available literature on the general subject of Internet and e-mail technology in local bookstores, and the public library. In a Barnes and Noble Bookstore in Alpharetta, Georgia, over different 75 books with Internet, e-mail or related titles were found, while at B. Dalton Booksellers in the same city, 42 such books were on the shelves. My local public Library, (Forsyth County, Ga.) possessed 23 such titles with 14 of them being available at the time of my investigation, while a neighboring public library (Fulton County, Ga.) had 43 related titles in the system with 19 available on the day of the search.

I selected three books from my local library to serve as basic introductory guides to the subject of electronic communication. These books were chosen based upon availability, content, format and what I perceived as reader friendliness.

The first book selected was the 1997 edition of The World Wide Web Unleashed, by John December and Neil Randall, which presented a rather comprehensive overview of the theory and background of electronic communications technology as that technology relates to the Internet and E-mail.

This book was highly technical and did not constitute an easy read, nor do I believe the authors intended it to be read from cover to cover, but that its 1346 pages serve as a reference. Designed to take any reader from whatever point of ability they may be, to a higher skill or knowledge level, this book would allow a beginner to become more technically advanced and a person already possessing an advance technical background can increase to an even higher level of proficiency.

The book was divided into five basic sections, with the first section being an introduction to electronic communication, the history of the Internet and e-mail, and how this system developed. In the second section, the types of hardware and software that are essential for Internet and e-mail operations was addressed. The third and fourth sections showed the reader how to navigate the World Wide Web, and the last section presented an explanation of how to create Web sites. At the end of the book, there were reference pages that contained a listing of Internet resources.

The second background text was helpful in understanding many of the technical terms used in electronic communication technology. This book, The Business Internet and Internets – A manager's Guide to Key Terms and Concepts, by Keen, et al., was a non-technical work intended to provide management level people a higher degree of technical understanding without the usual technical jargon and terms. Written in such a manner that at any point, no prior knowledge was assumed, this book made an ideal cross-reference to the more technical World Wide Web Unleashed. An informative portion of this book was a selection of case histories of how the use of Internet and e-mail technologies has made measurable changes in various private corporations, affecting the way they do business.

The last of the three selected background texts was The Internet – Complete Reference 2nd Edition 1996 by Harley Hahn, which covered much of the same information as the two previous works, but in a format that was ideal for casual reading. Divided into twenty-eight non-sequential chapters covering various aspects of Internet and e-mail use, this book, though slightly dated, was comprehensive without actually being a technical manual. Of the three books used for background technical knowledge that allowed this paper to proceed, this was the one that seemed to be the most organized and well written and hence the most useful. Of particular interest, and not found in the other books, was a guide to abbreviations, jargon and common slang used on the Internet and in e-mail.

Through professional contacts, an organization called the Society for Human Resource Management (SHRM) was located. This organization, located in Arlington, Virginia has published a series of white papers, among these were E-mail Policies: Avoiding Accidents On The Electronic Highway by Michelle N. Martinez, E-mail In The Workplace: How Much Is Private? by D. Michael Underhill and Thomas Linthorst, and Electronic Communications In The Workplace: A New Challenge In Employment Law, by Susanne Peticolas and Kerrie Heslin. These white papers are available to members only, and are part of an ongoing effort by this organization to inform and advise managers of developing trends within their professional arena.

Another professional organization called the International Personnel Management Association (I.P.M.A.) provided several key documents including Eye on Employees, by Eleanor Trice, Director of Personnel Research for the I. P. M. A. This paper gave results of several recent employer surveys on the subject of employee monitoring of employees.

Another useful paper provided by the I.P.M.A. was Computers and the Law by Howard L. Meyer. The purpose of this paper was to examine the degree and nature of privacy rights that an individual may have with respect to electronic mail (e-mail) communications. At the outset, the paper tried to emphasize that e-mail does not have the same privacy protection as does regular mail because it does not enjoy federal status or the comprehensive protections which exist under the law. The paper focused on a number of different settings in which e-mail may be used, and discusses the privacy protections in each setting.

An inherent problem involving research on the internet is that the multitude of websites that are available are so quickly and easily changed and sites tend to come and go with unpredictable regularity. A source used in research could be updated after the researcher accessed the information, significantly changing the data. It is not uncommon that the website may no longer exist by the time the research is published, but unlike an out of print textbook or periodical, when a website is closed, it may leave no trace or history that can be referred to.

In any research, you must always consider the original source of the information, the accuracy of the information, the credibility of the author, the degree of documentation, and the objectivity of the information. This becomes difficult when doing research on the Internet. The above factors may not be apparent or discernable.

Not withstanding the above difficulties, research on the Internet opens many avenues that were either closed to most researchers or that make research logistically easier, such as reducing field research or eliminating trips to specific libraries. As an aid to readers of this research paper who may be viewing it on a disk and monitor, the www. portion of the following website addresses will not be given. This will prevent inadvertent accessing by hyperlink.

Well over 100 websites were investigated under search names such as "Internet," "Content Blocking," "Filtering," and "Monitoring," as well as combinations of the above. The following websites were most helpful in researching this paper, either by providing direct and usable data or quotes, or by supplying important background material.

The Global Internet Liberty Campaign is a coalition that says it is working for privacy, freedom to speak and to access information. It is opposed to any form of Internet blocking. Another group that opposes any form of content blocking or mandatory ratings is Cyber Rights and Cyber Liberties, an English group that has released a number of reports that support their viewpoint.

The website of the American Civil Liberties Union, The ACLU, also deals with this subject with reports on relevant court cases and several position papers. A site named Computer Professionals for Social Responsibility deals with technology and social issues and also takes an anti-blocking position.

A group that openly boasts that one of its goals is to counter and oppose any form of religious expression in public is People for the American Way. This group has been a primary plaintiff in several lawsuits against content blocking of pornography in public libraries.

A major website that explores the issue of Internet content blocking is the American Library Association, (ALA) sponsored by the organization of the same name has taken a stand against any forced use of content blocking in public libraries. Also holding to an anti-blocking viewpoint were the Electronic Privacy Information Center, Internet Free Expression Alliance, Center for Democracy and Technology,

A website that was amusing, as well as informative to explore was Peacefire. This was among the most radical anti-blocking sites found. It uses case histories and news reports to make its case and includes an interesting section that gives specific instructions on how to override the various content blocking software. It was of particular interest that the details of how to block Surfwatch was blocked by computers using Surfwatch software, but the override instructions of other manufacturers were left unblocked.

A site funded by the Family Research Council that reflects a conservative, pro-family point of view is Filtering facts. It presents a variety of arguments for the use of blocking software. Also promoting content blocking was a site called Eight is Enough, which states its case through case histories and position papers.

The National Law Center for Children and Families, directed by Bruce Taylor, who wrote the Communications Decency Act, which was passed by congress but overturned by the Supreme Court, issues interpretations of legal matters, including content blocking, to non-lawyers. The anti blocking positions of the American Library Association are directly countered by a group called Family Friendly Libraries which deals with the issued raised in the A. L. A. website.

Other websites that hold a viewpoint in favor of content blocking were Cyber Angels, Enough is Enough, Integrity Online, Internet4Families, Speak Responsibly, the Family Research Council and the Green Ribbon Campaign.

Several persons were helpful in providing personal attention and providing answers to questions regarding this research paper. Among them was Brian Patton, of the City of Alpharetta Department of Community Development, who provided a vast amount of background material regarding the City of Alpharetta's current economic and business climate.

Of assistance also was Robert Mullis, Director of the Information Services Department, of the City of Alpharetta who provided information regarding the computer systems and software currently in use by the City.

Peggy Phister, Computer Specialist at the National Emergency Training Center in Emmitsburg, Maryland, contributed to this work by giving background data and policy information regarding the N.E.T.C. polices and procedures for electronic communication and blocking software.

Procedures

To solve any problem, it is necessary to first define the problem, then survey the history of the problem, including how it evolved and how others have dealt with similar problems. Relevant facts regarding the problem should then be researched and analyzed. Finally, using the compiled research, a proposal or solution is formulated.

In the introduction, the problem identified was that with the spread of electronic communication technology, there is an increased potential for conflict between an employee's perceived right to communication privacy and free speech versus the desire of the employer to support a controlled and productive work environment.

To support this point, an examination was made of data from professional, business, religious, legal and political organizations that have an interest in issues involving employee rights. Among these organizations, were the Society of Human Resource Managers, International City / County Management Association, the American Civil Liberties Union, the American Family Association and the manufacturers of various types of content blocking software.

This data presented an overview of the problems, costs, and possible solutions regarding employee Internet and e-mail abuse. These documents also presented case histories of attempts by employees and employers to achieve legal victories. These case histories demonstrated both successes and failures.

Personal interviews were conducted with the Manager of the Management Information Services Department of the City of Alpharetta. Historical and population data was obtained by reviewing the records of the Community Development Department and interviewing that agencies representative.

To determine the opinions and beliefs of the employees of the City of Alpharetta Department of Fire and Emergency Services a benefits questionnaire was distributed. This questionnaire dealt with employee perceptions and attitudes regarding Internet and e-mail usage. There were 57 completed questionnaires, out of 70 employees.

To learn what local circumstances other area local governments were currently operating under, a telephone questionnaire was called to 11 neighboring city and county governments regarding their Internet and e-mail policies. The questionnaire was limited to four questions to guarantee maximum participation. These questions were; Do you have specific policies regarding Internet and e-mail usage? Do you use any type of content blocking system on your computers? Do you monitor employee usage of electronic communication? Have your employees been given an opportunity to sign a form stating that they are aware of these policies.

Some information obtained from organizations with opposing views contained apparent contradictions. In most cases, these contradictions seemed to lean toward supporting the particular viewpoint of the reporting organization. Often such variations were minor, such as a matter of a few percentage points, and in the absence of any other standard, the most recent of the conflicting data was used. When there seemed to be a major discrepancy between facts presented by various organizations attempts were made to find independent sources.

It was not the intention or scope of this research paper to deal with technical aspects of electronic communications. Many works on this subject are currently available (see Literature Review), however for the sake of standardization of terms and word usage the following definitions and descriptions of nomenclature are provided.

The World Wide Web (WWW) is the global network of computers used for communication, entertainment, and information storage. They include computers used by businesses, schools, colleges, and individuals. Anyone with a home computer and modem is a part of the World Wide Web.

The Internet is the worldwide network of websites. The Internet is often used synonymously with the term World Wide Web. In order to access the Internet you must use an Internet Service Provider (ISP.) The ISP charges a monthly fee for their services.

ISP’s provide a tool known as “Web browsers,” which is a product such as Netscape Navigator or Microsoft’s Internet Explorer that displays prints and downloads documents. Each document on the Internet has an address that allows user to find and lock into any web-site in the world.

A variety of systems called "search engines" allow users of the Internet to search for desired information among all the web-sites that are part of the Internet. Services such as Yahoo, Magellan, Alta Vista, Lycos, Infoseek and others, provide this tool. Once a user has accessed the search engine, they simply type a word or combination of words which form a search request and the search engine provides a list of matching or near matching sites.

A Web Site or Domain Name is the Web address. This is the term that most people use when talking about web sites. Examples are www.hotmail.com and www.micosoft.com . A person might say "go to Firehouse and get an update" when they mean "go to www.firehouse.com and get an update." Generally, a domain ending lets you know what type of web site you are visiting, for example, .com would be a commercial site, **.**edu would be an educational site, .net would be a network site and .gov would be a government site. Sometimes this is a two-letter code indicating the country of origin, such as .ca for Canada or .au for Australia.

E-mail (Electronic Mail) is used to send messages from one computer to another. These messages are sent through e-mail addresses. These addresses have 2 parts, the user name and the domain name. They are separated by the @ (at) sign. E-mail may be a part of an Internet system or it may be separate and unconnected to the Internet.

This research was limited in a number of factors and assumptions. The parameters were deliberately limited to polices and procedures which are enforced by local and county government as contrasted to policies and procedures in the private sector.

It was not within the scope of this research paper to investigate the decision making process behind what sites to block, such as the current policy to block real estate categories but not automobile categories or the reasons for blocking Police Officers from accessing categories about drugs or firearms. This paper also will not consider the issues raised by title VII of the Civil Rights Act regarding possible religious discrimination incurred by the policy of allowing access to religious sites but blocking sites involving astrology and mysticism.

Local data involved the northern metropolitan Atlanta area and was obtained through original research. It was based upon the good faith assumption that the respondents to the telephone survey provided accurate information, further, local data may not reflect conditions in other geographic areas. Due to the constantly changing legal environment, new laws or court decisions may render any portion of this research invalid.

Results

Three questions were asked in the introduction to this research paper. The first was what is the nature, scope and cost of Internet and E-mail abuse in the workplace? The second was does an employer have a legal right to restrict, monitor, filter and control employee Internet and E-mail usage and are there limits to these rights? The last was what would constitute a fair, reasonable and legally enforceable policy regarding Internet and Email abuse in the workplace and what basic elements should be included in such a policy? .

According to a study of employee usage of internet and e-mail systems during the first three months of 1998, conducted by Spyglass Inc., manufacturer of Surfwatch Blocking Software, as much as 25% of employee online time was not work related. This was an increase over the 18% of non-work related online time in a similar study conducted by this company last year. This year, in an update of that survey, employee misuse was up 15% to 30%. Results for the first quarter of 1999 show that nearly one-third of employee Internet use was not work-related. This is double the amount of recreational surfing measured in the first quarter, 1998" (SurfWatch, May 11, 1999.)

The categories of abuse have not changed significantly, although the amount of time spent in those categories has doubled. Interestingly, the top two categories most frequently abused had reversed. Workers are now surfing more for news and investments than for sex. Visits to sexually explicit sites in first quarter 1999 dropped nearly 50% from 6.05% to 2.92%, while general news sites quadrupled from 2.01% to 8.76% of non-work-related surfing. The most popular categories of Web sites visited in order were; general news, investment, sexually explicit, travel, sports and entertainment. In the first quarter 1998, the most popular categories of Web sites visited in order were: sexually explicit, general news, entertainment, travel, sports, and investments" (SurfWatch, May 11, 1999.)

According to Theresa Marcroft, director of Marketing for SurfWatch. "Corporate America is spending $3.5 billion annually for Internet access. If 30 percent of that, or

$1.05 billion, is wasted on recreational surfing, companies will want to take notice and begin setting parameters for how the Internet is used during work hours." (SurfWatch, May 11, 1999.)

It is the policy of the City of Alpharetta Department of Fire and Emergency Services to generally not engage in employee surveillance, other than as it relates to Internet and e-mail usage. To investigate employee perceptions regarding this issue, I conducted a confidential (blind) survey of 57 out of 75 employees. This survey had two questions. Do you occasionally or frequently use the Departments e-mail and Internet for non-work related purposes and have you been informed of the Departments policies regarding the use of the e-mail and Internet for non-departmental purposes? The results of this survey were that 38 of 57 employees admitted that they do occasionally or frequently use the Departments e-mail and Internet for non-departmental purposes. When asked if they had been informed of the policies regarding the use of the e-mail and the Internet for non-departmental purposes, 31 of 57 said no, and 19 were aware that policies existed but did not remember seeing them in writing or hearing them discussed by their supervisors. Only eight employees said they knew of and understood the policies. Several employees expressed the opinion that if there were policies, they were only for show and would never be enforced. All 57 employees surveyed were aware that the City of Alpharetta employed a content blocking system, but of these, 28 were unaware that a user log was generated by that system and a record of usage and attempted access to blocked sites was maintained.

The use of passwords or log-in codes can lead employees to the mistaken assumption that communications carried by these methods are private and confidential.

Despite the appearance of privacy, the owning agency (City, County or State,) can and often will monitor, document, and record employee communications. Voicemail messages can be stored automatically and most Internet programs regularly back-up documents. On networked systems this backing up of documents may take place in a room or building remote from and inaccessible to the original user.

The monitoring of electronic communications by employers is more commonplace than many employees seem to believe. Of 301 businesses and industries of various sizes surveyed by MacWorld magazine, 21 percent of respondents (30 percent in large companies) "engaged in searches of employee computer files." Almost 16 percent report having checked computerized employee work files, and 9 percent have searched employee e-mail (MacWorld Magazine, 1999.)

Is the City of Alpharetta acting within its legal rights when it blocks and reviews e-mail, and Internet exchanges? The issue between an employee's right to privacy and confidentiality and the employer's right to monitor the use of the electronic media that it owns, has been at the heart of a number of court decisions (SHRM Legal Report, Winter 1999.)

Some fire service employees may fail to realize that the various forms of electronic communications such as e-mail and the Internet, when placed in the station or headquarters facility by the governing agency are the property of that department and therefore under that departments full control. The use of passwords or log-in codes can lead to the false assumption that these communications are private and confidential. Regardless of the employees assumption, the owning department (City, County or State,) can monitor, document, and record their employees' communications.

The Fire Chief or other government official is acting within their legal rights when they review e-mail, and Internet exchanges. The issue between an employee's right to privacy and confidentiality and the employer's right to monitor the use of the electronic media that it owns, has been at the heart of a number of court decisions (SHRM Legal Report, Winter 1999.)

Among the issues addressed were whether an employee has a reasonable expectation of privacy regarding electronic communication in the workplace. In deciding these cases, the courts have generally asked several basic questions. The first two questions are whether the employer had an established policy against personal use of the Internet and e-mail, and whether the company ever disclosed to employees that e-mail messages are automatically stored and could be accessed by supervisors. Another question the courts have asked employers is whether employees had been provided an opportunity to sign a form, acknowledging that e-mail was to be used for business purposes only and that usage would be monitored (SHRM Legal Report, Winter 1999.).

In cases where the employer was able to document that they met the above standards, the courts have generally held that they do indeed have a right to monitor employee electronic communications. This is most often based upon the principal that these communications which are conducted on employer owned equipment are therefore part of the company's property (SHRM Legal Report, Winter 1999.)

The only federal statute, that specifically addresses interception of electronic communication in the workplace, is the Electronic Communications Privacy Act (E.C.P.A) of 1986, which amended the Omnibus Crime Act of 1968. This statute expanded existing prohibitions on the unauthorized interception of wire and oral communications, to include electronic communications as well. In general, the statute makes it illegal to intentionally intercept another's electronic communication, where the interception occurs on the premises of a business affecting interstate commerce. The statute provides for substantial civil and criminal penalties.

One important factor considered by the courts is that the ECPA only applies to electronic communications which "affect interstate commerce." Therefore, internal company communications limited to a single state, this also includes local government agencies, are exempted from the law. Second, the "business use" exception allows anyone "whose facilities are used in the transmission of a wire or electronic communication… to intercept, disclose or use that communication in the normal course of his employment while engaged in any activity which is a necessary…to the protection of the rights or property of the carrier" (SHRM Legal Report, Winter 1999.)

Finally, the "prior consent" exemption protects a company from liability when "one of the parties to the communication has given prior consent" to the interception or disclosure. Courts have found this exemption satisfied by both expressed and implied consent by employees. Finally, ECPA does not prevent access to electronic communications by system providers. It has been argued that an employer who maintains its own e-mail or voicemail system should qualify as a system provider (SHRM Legal Report, Winter 1999.)

In the case of Borland International versus Symantec Corporation, Symantec hired a high level Borland employee. It was alleged that just before the employee left Borland, he e-mailed confidential and proprietary material to Symantec and its President. A criminal investigation commenced and company and personal computers at Symantec and at the home of its president were searched. The courts ruled for the rights of Borland International to protect and retrieve their property (Borland v Symantec.)

In Bourke v. Nissan Motor Co*.(1991),* two systems administrators alleged that their privacy had been violated when their supervisor read their e-mail. The e-mail contained jokes, offensive material and criticized the supervisor. As a result, the employees were fired. The court ruled that since the company owned the e-mail system, it had the right to read any e-mail (Bourke v. Nissan Motor Co.)

In Alana Shoars v. Epson America Inc. (1994), a supervisor was directed by Epson to tell employees that e-mail was confidential. Later she determined that her own e-mail was being read by her supervisor. When she complained, she was fired. She sued under a California statute prohibiting illegal wiretapping. The case was dismissed (Alana Shoars v. Epson America Inc.)

In the case of Flanagan v. Epson America Inc. (1991), a class action suit was filed on behalf of all employees whose e-mail had been systematically read. The California court held that the state statute was not intended to protect electronic communications such as e-mail and that the federal Wiretapping Act also did not apply because the interception was done with employer equipment. This case was also dismissed (Flanagan v. Epson America Inc.)

Finally, in Thomason v. Bank of America (1995), an employee was fired after the employer discovered e-mail messages which revealed that the employee worked as a professional gay stripper. The courts ruled in favor of the employer (Thomason v. Bank of America.)

Among the issues addressed in these and other cases are whether an employee has a reasonable expectation of privacy regarding electronic communication in the workplace. In deciding these cases, the courts have generally asked several basic questions. The first two questions are whether the employer had an established policy against personal use of the Internet and e-mail, and whether the company ever disclosed to employees that e-mail messages are automatically stored and could be accessed by supervisors? Another question the courts have asked employers is whether employees had been provided an opportunity to sign a form acknowledging that e-mail was to be used for business purposes only and that usage would be monitored (SHRM Legal Report, Winter 1999.)

In cases where the employer was able to document that they met the above standards, the courts have generally held that they do indeed have a right to block and monitor employee electronic communications. This is most often based upon the principal that these communications which are conducted on employer owned equipment are therefore part of the company's property (SHRM Legal Report, Winter 1999.)

Another consideration in this area is that an employer may not be the only person looking at the employees e-mail. Anyone who has computer knowledge may be able to bypass codes and read any persons e-mail. It is also a fact that the service provider can monitor your e-mail without your knowledge (Garcia.)

Fire service employees must be made to realize that e-mail and the Internet, when placed in the workplace by the Department are, like other apparatus, the property of that Department. The right to set policies and procedures for the use of that equipment is the right of the owning agency. Further, they must understand that the owning agency (City, County or State) has a legal right to monitor, document, and record their employees' communications when agency owned electronic communication systems are used.

In an effort to ascertain the policies of local governments in my area (Greater metro Atlanta,) a survey was made of the Management Information Services (or equivalent) departments of selected local City and County governments regarding their Internet and e-mail policies. This survey asked three questions: Do you have specific policies regarding Internet and e-mail usage? Do you use any type of content blocking system on your computers and is this system monitored? Have your employees been given an opportunity to sign a form stating that they are aware of these policies? A fourth question, was originally intended, “have you had any incidents or problems involving the use of the Internet or e-mail systems within your organization?” However, the Assistant Director of the City of Alpharetta Human Resources Department recommended that this information was of such a sensitive nature that for legal reasons the respondents might not wish to answer (B. Busby, Department of Human Resources, personal communication, June 1999).

In regards to the first question, it was found that every local government that responded to the survey had some type of policy in place regarding employee use of the Internet and e-mail. Inherent in each of these policies were limits on personal usage by employees.

The answers to questions two and three are illustrated in the following table.

Table One

Survey of Internet and E-mail Policies of Selected Local Area Governments

	Question #2	Question 3	Question #4
City of Decatur (404-373-4100)	Yes	Yes	Yes
Douglasville (770-920-3001)	Yes	Yes	No
Duluth (770-476-3434)	No	No	Yes
Lawrenceville (770-963-2414)	Yes	Yes	No
Marietta (770-794-5530)	Yes	Yes	Yes
Peachtree City (770-487-7657)	Yes	Yes	No
Roswell (770-641-3727)	Yes	Yes	No
Smyrna (770-434-6600)	Yes	Yes	No
Cobb County (770-499-4444)	Yes	Yes	No
Dekalb County (404-371-2000)	Yes	Yes	No
Fulton County (404-7300-4000)	Yes	Yes	No

These results show that the nature, scope and cost of Internet and e-mail abuse in the workplace is significant, but an employer does have a legal right to restrict, monitor, filter and control employee Internet and e-mail usage. These results also demonstrate that the City of Alpharetta Department of Fire and Emergency Services does have reasonable cause for concern regarding potential employee misuse of the Internet and the e-mail systems. The enforcement of existing policies, the continued use of content blocking software and increasing the monitoring of employee usage may reduce these concerns. However, as demonstrated, even though many city and county governments commonly use content blocking software, monitor e-mail usage and generally have policies regarding such Internet and e-mail usage, these policies may not meet the requirements of the courts regarding employee training and acknowledgment or in adequately of documentation.

Discussion

Scientific and technical developments in the private sector often tend to outpace developments in the fire service. When new developments are eventually integrated into the fire and emergency system, fire service managers can be slow to develop and refinethe policies and procedures that these developments may require.

Over the past few years, electronic communication technology, such as e-mail and the Internet have become a basic tool in both inter-office and intra-office communication for the private sector. E-mail allows workers to communicate with each other, as well as with other outside the business, while the Internet provides information quickly and efficiently.

At the same time, the Internet and e-mail can pose new problems for Fire Chiefs. One problem is the belief, on the part of the Chiefs, that the Internet and e-mail can distract employees who may prefer to spend work time surfing the net, communicating with colleagues or friends, or playing computer games. Consequently, chiefs feel they have a vested interest in supervising employee Internet and e-mail usage.

Other chiefs may have legal and liability concerns. Misinformation can often be unknowingly but quickly disseminated when it is sent via e-mail. Messages that were thought by an employee to have been erased can end up as evidence in criminal and civil law suits. Examples might include messages sent by an alleged harasser, or confidential communications between the Fire Chief and the Human Resources Department involving a planned disciplinary action (Underhill and Lintherst.)

Yet another issue for a Chief to consider is the use of the Internet and other computerized communications to sexually harass and discriminate employees or to be used by employees for other illegal or unethical activities. In such a case, the employer could be held to varying degrees of liability, charged with discrimination or accused of a hostile work environment. At least one court has recognized that the Internet could be considered a "workplace" for the purpose of holding an employer liable for sexually harassing employee conduct on the Internet (S. H. R. M. Legal Report winter 1998.)

Can the Fire and Emergency Services in general benefit by using these electronic communication technologies, and more specifically, can the City of Alpharetta Department of Fire and Emergency Services benefit? This research paper has identified several areas of direct application where emergency services can be improved by this technology.

Among those identified are instant written communications, the sharing of ideas and techniques across regional, state, and national boundaries, the sending and receiving of files and documents, and professional research through various web-sites. Perhaps most important to the fire service, professionalism can be enhanced when employees routinely access special interest web-sites that provide news and features that would not be carried in the popular media. Another advantage of the World Wide Web is that it is also inexpensive to use.

According to a Society of Human Resource Management Legal Report, there are however, a number of problems inherent with computerized communications which an executive fire officer must be aware. Not only can there be supervision concerns, such as cost and time management, but there are some legitimate liability issues that can affect policy decisions (SHRM Legal Report, winter 1999.)

One issue of concern to the employer is that Internet and e-mail communication are often less structured than formal, written letters. Employees often send messages in a casual style and may be tempted to include comments in e-mail that they would never consider putting on paper. Further, the ease with which Internet and e-mail messages or images can be distributed to large groups at the touch of a button could mean more people can be affected by a single correspondence. This also increases the possibility of the release of confidential or legally protected information to third parties. Additionally, the speed with which messages can be sent increases the likelihood of misdirected communications (SHRM Legal Report, Winter 1999).

Some employees mistakenly believe that a deleted e-mail or Internet message is destroyed forever. Due to the current level of technology however, this is not often the case. This ability to retrieve deleted messages can create problems for the employee as well as the employer in, for example, a legal action.

Other concerns that a Chief might have, is that the system could be at risk to receive computer viruses, that someone could intercept transmissions which might include sensitive information, or even that disk storage will be filled with non job-related clutter, that has been down-loaded from the Internet. Finally, not to be ignored is the concern that the user may be tempted by the opportunities of the Internet into spending work time on non-productive or non-job related activities (The Complete Idiot's Guide to the Internet.)

The unique features of the Internet and e-mail explain why litigation surrounding their use or misuse appears to be increasing. With this increase, comes the need for executive fire officers to consider enacting new policies and procedures or at least revisiting existing policies and procedures to consider revisions

In an effort to overcome some of these issues, employers are increasingly turning to another new technology, blocking software. This software is designed to prevent access to certain websites. It is installed on individual computers or on networks of computers and works with a web browser to block certain information or sites that would otherwise be available. A growing use of this technology is by business wishing to prevent illegal or potentially offensive use of the Internet, or simply to enable workers to focus upon their job.

Some blocking software prevents access to sites based upon standards provided by the vendor while others allow the end user to specify what may or may not be accessed. The nature and degree of blocked sites can vary from system to system. Blocked categories often include hate speech, criminal activity, sexually explicit language, “adult” topics, and violent speech. It is possible to also block religious, political, sports, entertainment and even news sites. If carried to an extreme, this software can block categories of expression that could be based upon ideological lines, such as liberalism/conservatism, pro-gun or anti-gun, feminism, pro-life/pro-choice, or gay and lesbian issues. Access could be allowed or denied to web sites that offer opposing views on these issues, based solely upon the point of view of the person controlling the system (The American Civil Liberties Union Homepage.)

One blocking software program called SurfWatch blocked access to the White House web site about the social lives of the President and First Lady and the Vice President and his wife. The page was called "couples.html", which made the software think it contained adult themes. When the site was renamed "principals.html" the problem was solved. In another incident, an article about SurfWatch software being purchased by the Archie R. Dykes Medical library was blocked and the library staff and visitors were prevented from browsing the libraries own Web site (Peacefire.Com.)

The American Family Association (AFA), a conservative religious organization, found that “Cyber Patrol,” blocking software, had placed them on its blocked list because of the group's opposition to homosexuality. This site was blocked under the category "intolerance," which was defined as "pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability or handicap, gender or sexual orientation." An AFA spokesman told reporters "Basically we're being blocked for free speech" (Peacefire.Com).

Another point of concern is about the technology itself. Blocked words and letters might include "XXX," intending to block adult oriented sites but which also may block Super Bowl XXX or "breast," which could prevent someone from entering a pornographic site as well as obtaining information about breast cancer. Another combination may block the consecutive letters "s," "e" and “x” which could block sites containing the words "sexton" and "Mars exploration," (Peacefire.Com.)

It is interesting to note that the National Emergency Training Center, which provides computer access to over 350 employees and 5000 students annually, does not use any form of blocking software. According to the N. E. T. C., there have been no problems with allowing unlimited access and no changes are planned at this time (Personal interview, Peggy Phister, Computer Specialist June 1999.)

The decision to bock or not to block should not be based upon a reaction to an isolated incident or a management fear that may or may not reflect actual use or abuse by the employee. Use of blocking software can be a useful tool, but should be considered as only a part of an overall management program.

Recommendations

The City of Alpharetta Department of Management Information Services (MIS) should continue to maintain the city wide computer network that includes an e-mail system and Internet access. This system is provided to assist in the conduct of the business of the Department of Fire and Emergency Services, and to facilitate the achievement of public goals and objectives. All computer hardware and software should continue to be the property of the City of Alpharetta, and under the operational control of the MIS Department but under the supervision of the department to which it is assigned. The issue of final authority regarding electronic communication policy matters should be decided in favor of the individual department head.

All purchases and replacement of computer hardware and software should continue to be the responsibility of the MIS Department who will be budgeted accordingly. No privately owned hardware or software should be installed or used in conjunction with the Internet or e-mail system.

The City of Alpharetta Department of Fire and Emergency services should develop a comprehensive training program regarding electronic communications. Clear rules must be established and communicated to employees regarding the use of profanity, obscenity, harassing, and defamatory language in departmental communications. Employees should be advised to follow the adage that "If you can't say anything nice, don't say anything at all."

This training of employees should include information about the departments accountability for its communications. Employees should understand that all communications leaving the department can be identified in terms of the agency's addresses and headers. Thus, any posting of a defamatory message on an external net may be viewed as reflective of the agency's position.

The department should develop rules and procedures regarding record retention. Employees should be instructed on how to purge and delete unnecessary files periodically.

Employees should be instructed regarding possible copyright infringement through use of the Internet. They must understand that original material is implicitly and immediately copyrighted. Copying of any existing copyrighted material may involve violation of copyright laws.

The department must ensure that employees are aware of the departments polices regarding monitoring and blocking. The fact that an employee knows that the employer has the capability of monitoring his or her work activity does not constitute consent. The department could present to each employee a written policy on monitoring, and the employee may be considered by the courts to have given implied consent, but a signed form regarding the matter would meet all court requirements. The City of Alpharetta Department of Fire and Emergency Services and the MIS Department must reserve the right to review, audit, intercept, access and disclose all messages created, received or sent over the e-mail system for any purpose.

All procedures regarding blocking and monitoring of the Internet and e-mail systems should be made known to the employees. It should however be the policy to base no personnel action on any personal or non-job related information that may be unintentionally be encountered or intercepted unless that information involves violations of the law. If the information obtained by monitoring is used in performance evaluations or for disciplinary purposes, the data collected through monitoring should not be the exclusive basis for a decision and the employee should have reasonable opportunity to rebut the charges. In no instance should it be the sole basis for a personnel decision. The department should periodically review the procedures governing blocking and monitoring to ensure compliance with new statutes and case law.

In keeping with its policy of employee empowerment, the members of the City of Alpharetta Department of Fire and Emergency Services should continue to be encouraged, when possible, to follow all departmental guidelines and accepted professional standards. However, each member, regardless of rank or assignment, must be empowered, to apply their best judgement, based upon experience, training or special knowledge of the situation, to make whatever decision or exception they deem most appropriate at that time. All exceptions to these electronic communication policies, as with other policies, should be made after considering if that exception is legal, moral, ethical, and safe. Also it must be asked if it meets the Departments mission and values, is the person making the exception willing to stand by their decision and is the exception in the best interest of the public and the City?

The City should provide to all employees through classroom and written format, information regarding all policies and procedures involving computer usage, as well as individual rights and responsibilities. Among this information, employees must be made aware that messages composed, sent, or received electronically is not the private property of the employee but are and shall remain the property of the City of Alpharetta. Employees should also be advised that e-mail systems are non-securable, the confidentiality of messages must never be assumed. Even when a message is erased, it is still possible to retrieve and read that message.

Currently, an employee is assigned an e-mail address upon hiring. No e-mail address, other than that assigned by the City of Alpharetta should be used by the employee to access e-mail on any city owned computer. All passwords used by an employee should be disclosed to the City or they should be rendered invalid. Employees should be advised that the use of passwords for security does not guarantee confidentiality.

While the City should not entirely prohibit the use of the e-mail system for personal communication, it should assure that such use be infrequent, conducted with a supervisor's knowledge and must not interfere with the employees assigned duties and responsibilities. Under no circumstances, should the e-mail system be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.

The employee must be made to understand that e-mail system must not be used to create any offensive or disruptive messages. Among those which could be considered offensive, are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin, or disability. Further, the e-mail system should not be used to send or receive copyrighted materials, employee personnel files, proprietary information, or material or documents that would normally and properly be handled with discretion.

All employees must be aware that any e-mail messages should be considered confidential by other employees and deliberately accessed only by the intended recipient. Employees, other than direct supervisors and members of the Department of Management Information Services should not be authorized to retrieve or read any e-mail messages that are not intended for them. Employees should not attempt to gain access to another employee's messages without permission.

Employees should be informed that while personal access to the Internet is not completely prohibited, it must be limited in scope, moderate in occurrence and under no circumstances can it be allowed to interfere with the employee’s normally assigned tasks and responsibilities.

Employees must also be informed that content blocking software is installed on all computers having Internet access. The City of Alpharetta does not in any way presume to tell its employees what information they may or may not access on their own time and while using their own computers. However, when the employee is using a City owned computer and doing it “on the clock”, the City has a clear interest and legal right to control and monitor the information accessed.

A master list of all attempts to access blocked sites will be maintained electronically throughout the network. This list will identify the site where access was attempted, the computer used, the time the access was attempted and the password used. The City is aware that there are many reasonable ways that a person could inadvertently make a hit upon a blocked site without improper intent. Only in cases where a clear pattern of misuse is established should any action be taken.

Any employee who knowingly violates these policies or who has established a clear pattern of misuse of the Internet or e-mail system for improper or inappropriate purposes, or who through the use of the Internet or e-mail brings controversy or scandal upon the City, should be subject to discipline, up to and including termination. After being made aware of these policies, employees should sign a statement that they have read the policies, have received a copy of the policies and have had a chance to discuss the policies with a supervisor. This form should state that the employee understands that the e-mail systems that are provided by the City of Alpharetta are to be used primarily for conducting official business. That they understand that use of this equipment for private purposes is discouraged. Further, they should agree not to use a password that has not been disclosed to the company. On this form they should also agree not to access a file or retrieve any stored communication other than when so authorized.

This form, signed by the employee should state that the City reserves the right to review, audit, intercept, access and disclose all matters on the City owned Internet and e-mail systems at any time, with or without employee notice, and that such access may occur during or after working hours. The employee should also acknowledge that they are aware that use of a city-provided password or code does not restrict the cities right to access electronic communications. Finally, the employee should sign that they are aware that any violations of this policy may subject them to disciplinary action, up to and including termination.

There are other guidelines for effective and appropriate use of the Internet and e-mail systems that should be included in employee training. Just as there are certain standards for business writing, e-mail communications have their own standards. Employees must be taught to assume that since all e-mail messages could be seen by anyone, they should write it with the same care as for a letter or memorandum. They should always check for errors in spelling and grammar. E-mail messages should be clear and concise framed in a way that allows the recipient to respond by simply saying yes, no or thank you.

Reference

Borland International, Inc. v. Eubanks, et al., Santa Cruz, CA, County Superior. Court. Civil. Case No. 123059 2.

Bourke v. Nissan Motor Co, No. YC003979 Cal. Sup. Court., Los Angeles County, 1991.

Cozzetto, D. & Pedeliski T. (1999) Privacy and the Workplace: Technology and Public Employment). International Personnel Management Association, Alexandria VA.

December J. & Randall N,, The World Wide Web Unleashed 2nd Edition (1997), Macmillan Publishing, Indianapolis, IN. USA,

Flanagan v. Epson America Inc No. BC007036, slip op. Cal. Sup. Court, Los Angeles County, March 12, 1991.

Garcia E. C. & Meyer, H. L., E-mail and Privacy Rights, Computers and the Law, (fall 1996) Society for Human Resource Management, Alexandria, VA.

Hahn, H. The Internet – Complete Reference 2nd Edition, McGraw-Hill, New York, NY, 1996.

Keen, W. Mougayar, W. & Torregrossa, The Business Internet and Intranets – A manager's Guide to Key Terms and Concepts, 1998 Harvard Business School Press, Boston, MA.

Kent, P. The Complete Idiot's Guide to the Internet, 4th Edition, Macmillan Publishing, Indianapolis IN. 1997.

Mac World, Mac Publishing, L.L.C. Apple Computer, Inc. (1999) Mac Publications. USA.

Peticolas, S. & Heslin, K. Electronic Communications In The Workplace: A New Challenge In Employment Law (March 1999) Society for Human Resource Management Legal Report, Society for Human Resource Management, Alexandria, VA.

Alana Shoars v. Epson America Inc. No. SCW112749 Cal. Sup. Court, Los Angeles County, (1989). Appeal denied, Supreme Court of California, June 29, 1994, 994 Cal. LEXIS 3670.

Thomason v. Bank of America 1995 Cal. LEXIS 1843, (March 15, 1995), appeal denied by Supreme Court of California

Sterling, B. History of the Internet, (1998) Bruces@wellsfca.us, Literary Freeware From: THE! F&SF Science Column #5"Internet."

Surfwatch in the News (Aug. 13, 1998.) SurfWatch Software Inc., a division of Spyglass Inc. Los Gatos, Calif. surfwatch.com.

Trice, E. Eye on Employees, (1997) International Personnel Management Association (IPMA,) Alexandria VA.

Underhill T. & Lintherst, T. A., E-mail in the workplace: How much is private? SHRM White Paper (February 1996) Society for Human Resource Management, Alexandria, VA.

Appendix One

The following is the existing City of Alpharetta Policy regarding the use of electronic communication technology. Note the absence of reference to monitoring and blocking of e-mail and Internet communications, inadequate definition of terms, absence of date of issue or revision, as well as the general vagueness of some prohibitions. This policy was distributed over the e-mail system and was not on City of Alpharetta letterhead and there was no indication of the identity or authority of the person who issued it.

City of Alpharetta
Information Technology Polices

Information Systems is responsible for the management and security of computer and telephone systems for the City of Alpharetta (COA). The intent of this document is to help its users create secure and reliable systems for City business. COA restricts access of these systems to City staff and companies and individuals with contractual relations with the COA. COA policies require that these persons use its information technology resources in a responsible, efficient, ethical and legal manner.

All computers, communications equipment and software owned and/or used by the City of Alpharetta is to be used solely for City-related business. Any commercial or personal use not expressly approved by City contract is prohibited.

Computers, communications equipment and software owned and/or used by the COA is maintained and/or managed exclusively by the Information Systems department or its designee. Computers, communications equipment and software owned and/or used by the COA shall not have any personal or commercial components loaded or attached except by express written permission from Information Systems. Any unauthorized components or authorized components found to be problematic will be removed. This includes (but is not limited to) computer hardware, computer software, cell phones, radios and pagers. The City is not liable for any damage or loss of personal components or data.

All computer software loaded on a city-owned computer will have a valid license in the possession of the current user of the computer or the Information Systems department. This would also include proper registration of shareware if kept beyond the evaluation period. Computers, communications equipment and software shall not be moved within, between or removed from City facilities except by Information Systems personnel or as expressly approved by Information Systems. Any intentional damage done to computers, networks, files or communications will result in disciplinary action as defined by the COA employment policies and procedures.

The following guidelines are to be observed:

- Screen savers will have appropriate messages and pictures for an office environment.
- Users are responsible for storing their files in designated, appropriate locations, deleting obsolete files, and archiving files no longer needed in active storage.
- Games are not allowed on any City computer, except with express permission from Information Systems and the department Director. Games will only be allowed where the job requires extended time in a City facility.
- Neither system administrators nor users may change, alter or delete files of other users without authorization of the creator or appropriate manager.
- Users are responsible for the security of individual accounts and passwords. A user sharing their account or password with another person can be held accountable for any unacceptable or illegal use of the account. Please do not post passwords. When setting passwords, users should avoid obvious choices easily guessed by others.
- Internet access will be given only to those employees whose job requires them to do research and with their Director's approval.
- Any computer or communications device used for obtaining or accessing pornographic material or accessing "alternative" or questionable Internet sites will result in disciplinary action as defined by the COA employment policies and procedures.
- Send e-mail only from your own computer account and e-mail address; never under the name of another user.
- Read and dispose of messages properly. Avoid retaining a large number of mail messages.
- Use e-mail only for appropriate reasons.
- Sayings, quotations and disclaimers are not allowed.
- Download large files during non-business hours to avoid network performance problems.
- Download software only with permission of Information Systems. Software licenses must be in the possession of the user or Information Systems.
- Create distribution lists for regular communications only with prior permission of the recipients.
- Any messages posted to electronic bulletin boards, news groups or other information services should be business-related and appropriate for the employee's job responsibilities.

- Forward or re-post communications only with the author's prior consent or implied understanding.
- Always spell check.
- Avoid verbal attacks.
- Remember that humor, satire and sarcasm are difficult to convey in written communications, and, as a result, are often misunderstood.
- In your standard greeting, use your first and last name and department. Include the option to zero out to an attendants
- If you will be gone more than one day, create and activate an alternative greeting which includes how long you will be gone.
- Answer voice mail messages promptly.
- Check daily and return calls promptly.
- Do not ignore calls and allow them to go to voice mail. Unless you are busy with someone or something important, all calls should be answered.